UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

59

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/884,722	06/19/2001	Louis Robert Litwin JR.	PU010135	2515

7590 03/16/2005

JOSEPH S. TRIPOLI
THOMSON MULTIMEDIA LICENSING INC.
2 INDEPENDENCE WAY
P.O. BOX 5312
PRINCETON, NJ 08543-5312

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/884,722	LITWIN ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1,2, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosner et al, U.S. Patent 6,636,968 in view of Dolan et al, U.S. Patent 5,604,801.

As per claim 1, it is disclosed by Rosner et al of a method for creating a secure sub-network on a public network wherein the public network includes a set and subset of devices (see abstract and col. 2, lines 56-67). The destination (subset) devices contain a first private key (col. 4, lines 43-46). A source (master) device (which is predetermined) communicates with the destination (subset) devices as shown in Figure 3. A second private key is selected by the source (master) device and a public key is computed based on the second private key, the second private key is known only to the master device (col. 5, lines 3-7). The public key is sent to the destination (set) of devices by the source (master) device (col. 5, lines 3-7,14-18). A shared encryption key is computed and requests any encryption of any subsequent messages between any of the destination devices comprising a subset of devices using the shared encryption key (col. 3, lines 40-60 and col. 4, lines 48-60). The teachings of Rosner et al are silent in disclosing of the use of an access card that has a private key stored thereon and is

scanned to for use in encrypted communications. It is disclosed by Dolan et al of a card containing a private key which is used for encrypted communications (col. 2, lines 54-64 and col. 4, lines 29-31). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a private key to a card so that the private key can be portable. Dolan et al recites motivation for the use of storing a private key on a card by disclosing that only the authorized holder of the security device, or smart card, would have authorized processing of the messages (col. 2, lines 55-60). It is obvious that the teachings of Rosner et al would have found the teachings of Dolan et al effective by means of protecting the private key so that only the authorized user of the security device would have authorized processing of the message as suggested by Dolan et al.

As per claim 2, the teachings of Rosner et al disclose of programming the destination (subset) of devices with two parameters and computing the public key and the shared encryption key based on those two parameters (col. 4, line 48 through col. 5, line 7 and col. 5, lines 22-34).

As per claim 8, Rosner et al discloses of a method for creating a secure sub-network on a public network wherein the public network includes a set and subset of devices being programmed with two number g and n (see abstract; col. 2, lines 56-67; and col. 4, lines 45-48). The destination (subset) devices contain a first private key (secure number) x (col. 4, lines 43-46). A source (master) device (which is predetermined) communicates with the destination (subset) devices as shown in Figure 3. A second private key y and computed public key $Y=g^y \bmod n$ is selected by the

source (master) device and a public key is computed based on the second private key, the second private key is known only to the master device (col. 5, lines 3-7,14-18). The public key Y is sent to the destination (set) of devices by the source (master) device (col. 5, lines 3-7,14-18). A shared encryption key, Z=g^xy mod n is computed and requests any encryption of any subsequent messages between any of the destination devices comprising a subset of devices using the shared encryption key (col. 3, lines 40-60; col. 4, lines 48-60; and col. 5, lines 24-31). The teachings of Rosner et al are silent in disclosing of the use of an access card that has a private key stored thereon and is scanned to for use in encrypted communications. It is disclosed by Dolan et al of a card containing a private key which is used for encrypted communications (col. 2, lines 54-64 and col. 4, lines 29-31). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a private key to a card so that the private key can be portable. Dolan et al recites motivation for the use of storing a private key on a card by disclosing that only the authorized holder of the security device, or smart card, would have authorized processing of the messages (col. 2, lines 55-60). It is obvious that the teachings of Rosner et al would have found the teachings of Dolan et al effective by means of protecting the private key so that only the authorized user of the security device would have authorized processing of the message as suggested by Dolan et al.

3. Claims 3-7,9, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosner et al, U.S. Patent 6,636,968 in view of Dolan et al, U.S. Patent 5,604,801 in view of Scheidt et al, U.S. Patent 6,490,680.

As per claims 2 and 3, the combined teachings of Rosner et al and Dolan et al are relied upon for computing session keys (encryption key z) used in communications between a source device and multiple destination wherein a card is responsible for storing a private key. The combined teachings fail to disclose requesting a MAC ID from the devices by a master device. It is disclosed by Scheidt et al of using MAC codes sent between two parties (col. 11, lines 44-49 and col. 14, lines 16-22). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been concerning with transmitting data and maintaining its integrity. Sheidt et al recites motivation for the use MAC codes by disclosing that a recipient receives a transmitted MAC code and then calculates another MAC code, if the values match, it knows that the message has not been tampered with (col. 14, lines 20-22). It is obvious that the combined teachings of Rosner et al and Dolan et al would have found benefits from the teachings of Scheidt et al in order to maintain that data was not tampered with.

As per claims 5 and 9, the combined teachings of Rosner et al and Dolan et al are relied upon for computing session keys (encryption key z) used in communications between a source device and multiple destination wherein a card is responsible for storing a private key. The combined teachings are silent in disclosing of imposing a time restriction on a card that is valid for only a predefined time period. It is disclosed by Scheidt et al that disablement occurs when a card is in the reader and there is an

inactivity period (predefined time) detected (col. 15, lines 20-40). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply protection means to guard against unauthorized usage. Scheidt et al discloses motivation for use of disabling user activity by reciting of maintaining security and privacy for data and managing authorization of users when data is at rest and in transit on the system (col. 1, lines 44-48). It is obvious that the combined teachings of Rosner et al and Dolan et al would have found this beneficial since the teachings of Scheidt et al is concerned with security and privacy.

As per claims 6 and 10, the teachings of Scheidt et al disclose of renewing a validity period with the card subsequent to the predefined time period (col. 9, line 64 through col. 10, line 18). Please refer above for the motivation benefits as recited by Scheidt applied to the combination of the teachings of Rosner et al and Dolan et al.

As per claim 7, Scheidt et al discloses of reissuance of credentials for a user by transferring them from a server upon payment (col. 10, lines 19-23). Please refer above for the motivation benefits as recited by Scheidt applied to the combination of the teachings of Rosner et al and Dolan et al.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Please refer to PTO-892

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

3/8/05

CR

March 7, 2005